NIGHTDRAGON

SPECIAL REPORT: CYBER LEADERS ON 2025 TRENDS AND 2026 OUTLOOK

Top cybersecurity leaders in the NightDragon Advisor Council provide perspective on 2025 trends and 2026 spending outlook

January 2026

Foreward

Now in its fourth year, this Special Report aims to provide a view into how cybersecurity priorities are evolving amid rapid technological change and an increasingly volatile global environment. Through surveying of our robust network of CISOs and cyber leaders in our Advisor Council, we aim to capture not only where cybersecurity stands today, but how risk perception, investment discipline, and innovation cycles are shifting over time.

The 2025 data reflects sustained commitment to cybersecurity investment. Nearly three-quarters of CISOs (72%) reported that their budgets increased or increased significantly in 2025, up from 64% the year prior. Just as notably, 84% said they did not decrease cyber spend in any area, reinforcing the view that cybersecurity is now foundational to enterprise resilience.

Looking ahead to 2026, expectations remain measured but constructive. More than half of CISOs (56%) expect budgets to increase or increase significantly, while 32% anticipate no change and only 12% foresee decreases. While more tempered than the optimism of 2022 and 2023, this outlook reflects a maturing market focused on optimizing spend, reducing complexity, and aligning security outcomes more closely with business priorities.

That focus is evident in both investment and risk priorities. Artificial intelligence emerged as the most frequently cited theme on both sides of the equation. CISOs highlighted growing concern around AI-powered attacks —alongside the need to secure AI models, data, and access. Beyond AI, leaders pointed to persistent risk areas including identity and data access, insider threats, supply chain risk, endpoint compromise, misconfigurations, compliance gaps, and operational technology security. Many CISOs noted that the biggest risks in 2026 are not entirely new, but intensifying as environments grow more complex.

As this fourth iteration makes clear, cybersecurity is entering a more pragmatic phase—defined by sharper prioritization, tighter integration, and a continued focus on resilience. We hope the insights that follow provide clarity and perspective as you plan for the year ahead.

Table of Contents

Introduction

The NightDragon Advisor Council includes more than 100 leading CISOs, cyber experts and former government officials. These leaders come from Fortune 500 and other large enterprise organizations from a variety of verticals, including national security, defense, healthcare, finance, travel, critical infrastructure and more.

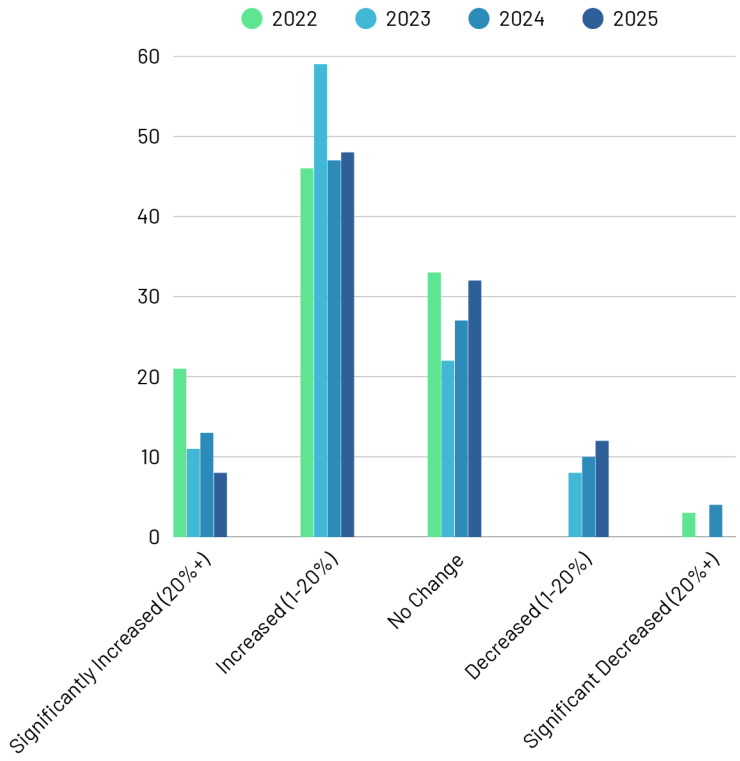
In this survey, Advisors anonymously provided input into spending trends for 2025 and 2026. They also provided insights into what risk areas concerned them the most last year, as well as what areas of risk they were prepping for in 2026. In this report, we will also dig more specifically into trends around AI, supply chain, and identity investment in dedicated sections. A select outline of the findings can be found below:

Findings

CISO spending remained positive in 2025, with 72% of respondents reporting that cybersecurity budgets increased or increased significantly—an improvement over 2024 that reinforces a multi-year trend of sustained investment. Meanwhile, only 8% of CISOs reported budget decreases, a level well below what would indicate broad pullbacks.

At the same time, the data points to a maturing spend environment. Flat budgets and modest decreases reflect tighter prioritization rather than retrenchment, signaling a shift from rapid expansion to more disciplined allocation as CISOs optimize spending heading into 2026.

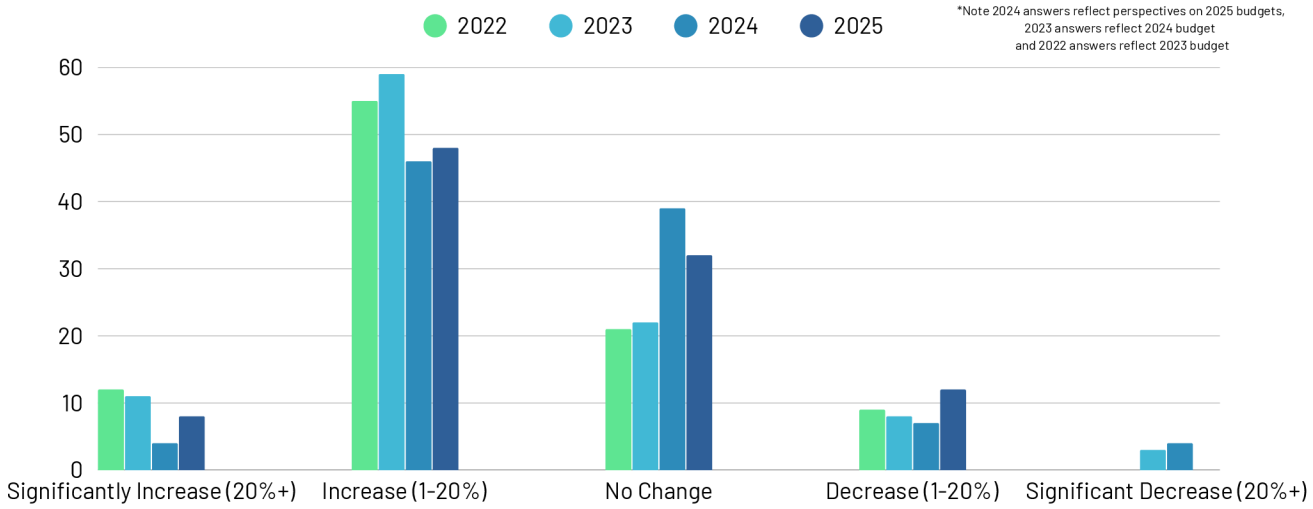
Did Your Cyber Budget Increase or Decrease YOY?



Are Cyber Budgets Going Up or Down?

CISOs' expectations for 2026 reflect cautious optimism. More than half of respondents (56%) expect their cybersecurity budgets to increase or increase significantly, up modestly from 2024 levels. While only 8% anticipate significant increases, overall growth expectations remain resilient, suggesting continued executive support for cybersecurity despite broader cost pressures.

At the same time, sentiment has become more balanced. Nearly one-third of CISOs (32%) expect budgets to remain flat, and 12% anticipate decreases—slightly higher than in prior years but still well below historical levels of concern. Compared to the stronger growth expectations seen in 2022 and 2023, the 2026 outlook points to a more measured planning environment, with CISOs prioritizing optimization and targeted investment over rapid expansion.



Where are CISOs Looking to Invest?

When asked what were the major categories they were looking to invest in in 2026, artificial intelligence emerged as the most consistent priority. Respondents cited a wide range of AI initiatives, including AI security, deepfake detection, AI-powered SOC operations, agentic AI deployment, and protections for AI models, data, and access.

Beyond AI, leaders said they will continue to invest in foundational capabilities such as application security, vulnerability management,

"The sophistication of attacks and the attack surface are expanding faster than organizations can defend themselves, so the investment in security continues to grow in order to keep up."

- Mike Rosen, CISO, iVerify

identity and access management, cloud security, supply chain, risk management, OT security, and resilience. Several noted that 2026 will be less about net-new spend and more about reallocating efficiencies to fund emerging priorities, particularly AI.

What Threats are CISOs Watching in 2026?

The threat landscape CISOs are watching in 2026 is characterized by heightened intensity across well-established risk areas, according to NightDragon Advisors.

Artificial intelligence is the most frequently cited concern, with leaders pointing to AI-powered attacks, deepfakes, AI-driven phishing, shadow AI, and the rapid spread of agentic AI as emerging challenges. These threats are layered on top of persistent exposure around identity, data protection, and endpoint compromise, particularly as attackers increasingly target data exfiltration ahead of ransomware or exploit misconfigurations to gain access.

Beyond AI, CISOs continue to flag third-party and SaaS risk, insider threats, and compliance gaps as risks that keep them up at night. Many noted that risks in 2026 closely resemble those of 2025, but with greater scale, speed, and operational impact, including increased focus on OT safety and resilience. Overall, the data suggests CISOs are prioritizing attack surface reduction, stronger identity and data controls, and improved threat and exposure management rather than anticipating entirely new threat categories.

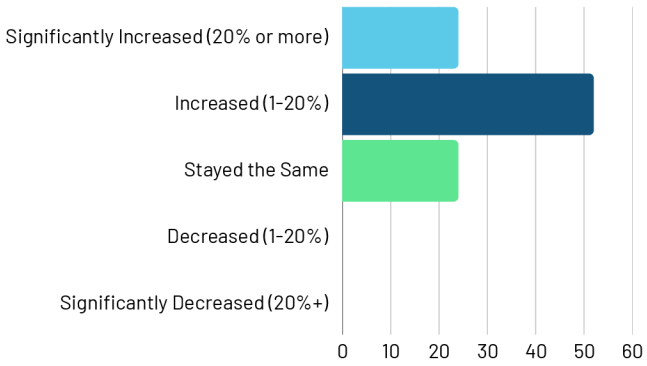
"With the recent AI adoption...across enterprises, new areas of risks continue to evolve. Traditional security was primarily revolving around the risks around human identities (employees), the assets they own (end point devices), or access they have (applications, cloud, servers, data)... However with the rapid adoption of AI and Agentic AI, human workforce is being replaced with agents with similar privileges and access and this will scale up more in the future... CISOs now need to relook the security strategy and programs to cover this new risk and specifically look for solutions to manage identities and privileged access for the agents, how to minimize data exposure and data leakage risks. All these are increasing the security spend not only in 2026 but also for next few years until we achieve maturity."

– George Eapen, Chief Technology & Security Officer, Abdul Latif Jameel

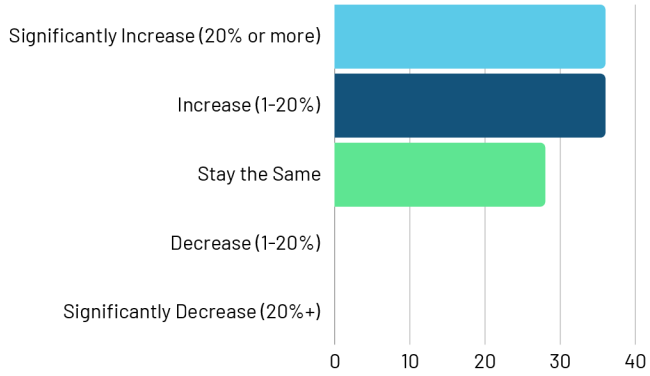
Our New AI Era in 2026

Artificial intelligence has moved decisively from experimentation to priority status within cybersecurity budgets. In 2025, 80% of Advisors said AI was a high priority, while the remaining 20% classified it as a neutral priority (none viewed AI as low priority). When it comes to spending, 76% of CISOs reported that AI budgets increased or increased significantly during the year, and no respondents indicating any reduction in AI-related spend.

AI Budget in 2025:



AI Budget in 2026:



The year-over-year change is particularly notable. In 2024, only 41% of CISOs reported increases in AI budgets, and a majority (59%) said spending remained flat. By 2025, 24% reported significant increases and 52% reported moderate increases, marking a sharp acceleration in both intent and execution. The data suggests that what was once exploratory investment has become operational.

Looking ahead to 2026, momentum is expected to continue. 36% of CISOs anticipate significant increases in AI budgets, with another 36% expecting moderate growth. "The investment in AI will continue to increase as it transitions from being part of organizational innovation to being part of the core security infrastructure," said iVerify CISO Mike Rosen.

Taken together, the data underscores a clear inflection point: AI is no longer a discretionary investment in cybersecurity, but a core pillar of how organizations plan to defend, detect, and respond to evolving threats.

Spotlight: Supply Chain

In the 2025 survey, 100% of Advisors expressed concern about supply chain risk: 40% reported being very concerned, 44% concerned, and 16% somewhat concerned. Notably, not a single advisor indicated low concern or no concern, underscoring the sustained urgency around supply chain threats following a steady drumbeat of incidents over the past year, including software update compromises, vendor credential abuse, and third-party service outages that cascaded across multiple customers simultaneously.

When asked to identify their biggest supply chain challenges, CISOs consistently pointed to a lack of visibility into vendor security practices as the primary constraint. Third- and fourth-party risk management and software supply chain vulnerabilities followed closely, underscoring how difficult it remains to assess upstream dependencies and inherited risk.

Several 2024 and 2025 incidents reinforced these concerns, particularly attacks that exploited trusted software components, compromised build pipelines, or leveraged excessive vendor privileges to move laterally into customer environments. Challenges around supply chain attack detection and response, vendor access and privileged account management, and regulatory compliance further compound the issue.

Geopolitical dynamics are adding another layer of complexity. Advisors cited geographic risk, restrictions on foreign software and vendors, and the impact of shifting trade and tariff policies as growing considerations in supply chain security decisions. In response, CISOs are increasingly moving away from static vendor assessments toward continuous monitoring, tighter access controls, and more resilient architectures—recognizing that supply chain risk is no longer episodic, but systemic.

Trends to Watch in 2026

Dataminr

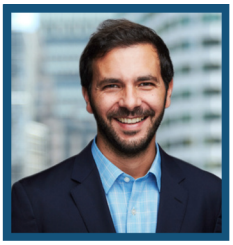
TED BAILEY, CEO, DATAMINR

BALAJI YELAMANCHILLI, CEO, THREATCONNECT

With cyber defenders drowning in alerts amidst growing threats and an expanding landscape, they are seeking intelligence that is specifically tailored to their business rather than generic threat feeds. In 2026, CISOs will demand tailored threat intelligence specific to their organization, the specific threats they face, and the security controls they have in place. They expect this information to be communicated in business terms, with risks, threats, and security investments communicated in financial terms.

Amid flat budgets and staff shortages, cyberdefense leaders must cope with rising waves of sophisticated attacks, including adversaries supercharged with AI technologies. They need to know what's happening in their environment without getting overwhelmed by information about the general threat landscape. They need to focus on whether their controls actually protect them from real risks, not theoretical ones.

Intelligence that can't answer "How does this affect my organization" becomes noise. 2026 will be the year organizations will begin moving beyond just consuming threat feeds to actively correlating external threat data with their internal control effectiveness to understand their real exposure.



ONAPSIS

MARIANO NUNEZ, CEO, ONAPSIS

After the unprecedented wave of SAP zero-day attacks in 2025—which resulted in more than 500 compromised SAP customers and over $1.2B in reported losses at a major global UK manufacturer—we expect 2026 to bring even greater adversary attention to the broader enterprise application landscape. Threat actors now clearly understand that systems like SAP, Oracle, and Salesforce hold the operational and financial heartbeat of large organizations, and manufacturing remains

Trends to Watch in 2026

one of the most exposed sectors due to its complex, highly interconnected environments.

In 2026, CISOs and CIOs will need to work more closely than ever to strengthen governance, visibility, and secure-by-design principles across these platforms. Organizations that treat enterprise application security as an operational imperative—not an IT task—will be best positioned to withstand the evolving tactics we've seen emerge over the past year.

CLAROTY

YANIV VARDI, CEO, CLAROTY

Digital transformation is booming—whether it's cloud migration or the acceleration of AI—and it's driving the exponential growth of cyber-physical systems (CPS). This is especially true in areas where the human workforce is being augmented or replaced with robotics and automation, such as Retail, Logistics & Warehousing, and Manufacturing. Nation-state actors and advanced ransomware gangs will increasingly target these hyper-connected environments, exploiting gaps left by immature or siloed security programs.

Consequently, we could see outages that ripple across supply chains on a national or global scale. As these risks mount, expect to see a stronger push, both from industry leaders and policymakers, for "secure by design" modernization and mandatory security frameworks to bring hyper-connected CPS environments in line with today's cyber-risk realities.

BLACKBIRD.AI

WASIM KHALED, CO-FOUNDER AND CEO, BLACKBIRD.AI

The cybersecurity world has shifted. Threat actors and nation states are operationalizing narrative warfare to target executives, companies, and countries. This is a new threat vector of 'Narrative Attacks' that are created by disinformation, misinformation, and deepfakes that cause financial, operational, reputational, and physical harm. The costs to create and execute these narrative attacks have collapsed and the consequences of them have exploded. To address

Trends to Watch in 2026

this new threat vector, cybersecurity leaders need to 'Know The Narratives' that are targeting their executives, company and industry, who the threat actors, influencers and nation states that are behind it, how fast is it scaling and spreading across networks, is it bot influenced, and what cohorts and communities are escalating it to do harm. Disinformation Security and Narrative Intelligence does just that, protecting organizations from narrative attacks so that they can make informed, actionable strategic decisions before, during, and after a crisis to significantly reduce risk.

HUMAN

STU SOLOMON, CEO, HUMAN

This year we hit a genuine inflection point as more than 50% of internet traffic is machine-based rather than human-driven, fundamentally reshaping our digital world. In 2026, machines will take the lead as the primary layer of digital interactions after a 6,900% increase in agentic traffic in 2025.

Agentic behaviors (like agents shopping, negotiating, or transacting on behalf of people) aren't a tomorrow problem, they're happening right now, expanding exponentially. This transforms the role of human oversight into an arm's length activity, empowering trusted agents to act on our behalf. Trust, authority, and accountability will take center stage in enabling these systems. Next year, businesses will need to focus on guiding trusted AI agents, and disabling the rest, in a world that's increasingly governed by machine-to-machine interactions.

NightDragon Perspective

As this year's survey makes clear, cybersecurity is entering a more disciplined and resilient phase. CISOs are operating with greater budget stability, sharper prioritization, and a clearer mandate to align security outcomes with business objectives. While the threat environment remains complex, the consistency of investment and the maturity of decision-making signal an industry that is no longer reacting to crisis, but building enduring capability.

From NightDragon's perspective, the pace of innovation, especially around artificial intelligence—is a source of genuine optimism. Across the ecosystem, we are seeing AI fundamentally reshape how security teams detect threats, respond to incidents, manage exposure, and secure increasingly dynamic environments. At the same time, the focus on securing AI itself reflects a healthy evolution in thinking: CISOs are no longer adopting new technology blindly, but demanding visibility, governance, and control as part of responsible innovation.

Looking ahead, we believe the most successful organizations will be those that pair technological advancement with operational rigor. The opportunity in front of the industry is not simply to deploy more tools, but to use innovation to reduce complexity, improve resilience, and stay ahead of adversaries moving at machine speed. NightDragon remains confident in the strength of the cybersecurity ecosystem and the leaders shaping it—and encouraged by the pragmatic optimism reflected in this year's findings as the industry prepares for 2026 and beyond.

Media Contact

NightDragon
Sarah Kuranda Vallone, VP Marketing
sarah@nightdragon.com